

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-154132

(43) 公開日 平成10年(1998) 6月9日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 15/00  
1/00

識別記号

3 3 0  
3 7 0

F I

G 0 6 F 15/00  
1/00

3 3 0 F  
3 7 0 E

審査請求 有 請求項の数15 O L (全 17 頁)

(21) 出願番号 特願平8-329586

(22) 出願日 平成8年(1996)12月10日

(31) 優先権主張番号 特願平8-259617

(32) 優先日 平8(1996)9月30日

(33) 優先権主張国 日本 (J P)

(71) 出願人 594057314

翼システム株式会社

東京都江東区亀戸2丁目25番14号

(72) 発明者 矢戸 広信

東京都江東区亀戸2丁目25番地14号 翼システム株式会社内

(72) 発明者 鶴村 亨三

東京都江東区亀戸2丁目25番地14号 翼システム株式会社内

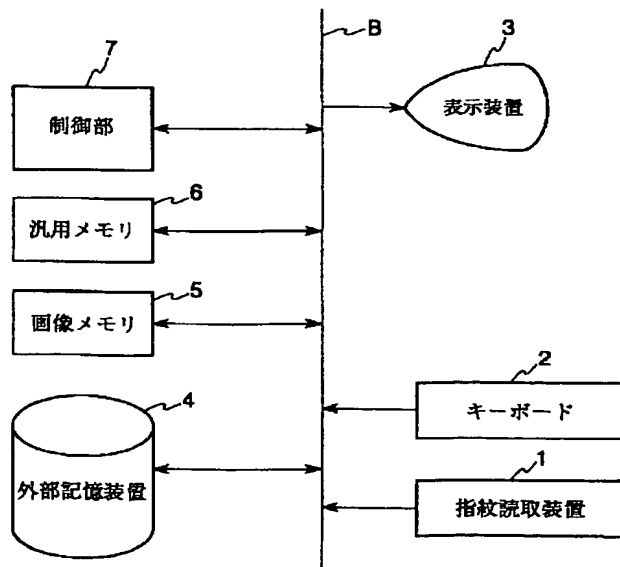
(74) 代理人 弁理士 木村 満 (外3名)

(54) 【発明の名称】 コンピュータシステム

(57) 【要約】

【課題】 ユーザに注意負担を強いことがないコンピュータシステムを提供する。

【解決手段】 外部記憶装置4によって、ユーザの指紋の画像に基づくコード化画像データが記憶されるとともに、当該ユーザからの指示によって処理を開始するか否かを示すデータが前記コード化画像データに対応させて記憶される。指紋読取装置1によって、ユーザの指紋の画像が読み取られる。キーボード2によって、ユーザから前記指示が入力される。制御部7によって、指紋読取装置1によって読み取られた前記画像に基づいて前記コード化画像データが生成され、当該コード化画像データに基づいて前記外部記憶装置4の検索がされ当該コード化画像データに対応する前記データが読み込まれ、前記処理を開始する旨のデータが得られた場合には前記処理が開始される。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項1】特定のユーザからの指示によってのみ開始する処理を実行するコンピュータシステムにおいて、ユーザの身体の一部の画像に基づくコード化画像データを記憶するとともに、当該ユーザからの指示によって前記処理を開始するか否かを示すデータを前記コード化画像データに対応させて記憶する記憶手段と、ユーザの身体の一部の画像を読み取る身体情報読取手段と、ユーザが前記指示を入力するための入力手段と、前記身体情報読取手段によって読み取られた前記画像に基づいて前記コード化画像データを生成し、当該コード化画像データに基づいて前記記憶手段を検索して当該コード化画像データに対応する前記データを読み込み、前記処理を開始する旨のデータを得た場合には前記処理を開始する制御手段と、を備えたことを特徴とするコンピュータシステム。

【請求項2】前記データはビットデータであり、前記記憶手段は、前記ビットデータを前記コード化画像データ毎にワード化したデータとして記憶すること

【請求項3】前記処理に対して各々番号が付されており、前記ビットデータのビット番号が前記番号と同一であることを特徴とする請求項2に記載のコンピュータシステム。

【請求項4】前記制御手段は、前記指示の入力があった時に、前記番号を指数として受け取り、当該指示を入力したユーザの身体の一部の画像を読み取る旨を前記身体情報読取手段に対して指示し、前記身体情報読取手段によって読み取られた前記画像に基づいて前記コード化画像データを生成し、当該コード化画像データに基づいて前記記憶手段を検索し、検索結果が得られた場合には、当該検索結果であるワードデータ中の前記番号をビット番号とするビットデータを抽出して戻り値とし、検索結果が得られなかった場合には、その旨を通知するデータを戻り値とするサブルーチンプログラムを実行すること

【請求項5】特定の操作者からの指示によってのみ開始する処理を実行するコンピュータシステムにおいて、操作者の身体的特徴を示す身体情報を記憶するとともに、当該操作者からの指示によって前記処理を開始するか否かを示す処理許可条件を前記身体情報に対応させて記憶する記憶手段と、

操作者が前記指示を入力するための指示入力手段と、前記指示入力手段からの所定の指示の入力に

前記取込手段により取込まれた身体情報に基づいて前記

処理許可条件を読み出し、前記指示入力手段により指示された処理を実行することが許可されているか否かを判別する許可判別手段と、を備えたことを特徴とするコンピュータシステム。

【請求項6】複数の処理について、操作者毎に身体情報と処理を認めるか否かを示す処理許可条件を記憶する許可条件記憶手段と、

任意の処理を指示する指示入力手段と、

前記指示入力手段により入力された指示に

より構成されることを特徴とするコンピュータシステム。

【請求項7】前記指示入力手段は、入力操作を検出し、入力の内容を含む検出信号を出力する手段を含み、前記許可判別手段は、前記検出信号をフックするフック手段と、前記処理許可条件に従って、前記フック手段によりフックされた検出信号が指示する処理が、前記操作者に許可されているか否かを判別し、許可されていると判別した際に、前記検出信号を前記処理手段に供給する転送手段と、を含み、

前記処理手段は、前記転送手段からの前記検出信号に

ことを特徴とする請求項5又は6に記載のコンピュータシステム。

【請求項8】所定のイベントの発生により開始され、操作者毎に処理を認めるか否かの別がある後続処理について、操作者毎に前記後続処理を認めるか否かを示す処理許可条件を記憶する許可条件記憶手段と、

入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶された処理許可条件を読み出し、前記後続処理を実行することが許可されているか否かを判別する許可判別手段と、

前記許可判別手段が、認められていると判別した際に、前記後続処理を実行する後続処理実行手段とを含み、前記許可判別手段は、前記所定のイベントの発生を検出して前記許可判別手段に制御を移行させるイベント検出手段を含む、

ことを特徴とするコンピュータシステム。

【請求項9】前記所定のイベントはファイル操作に関するイベントであり、

前記後続処理は、ファイルの操作を含む処理から構成される、

ことを特徴とする請求項8に記載のコンピュータシステム

ム。

【請求項10】複数のファイルを記憶するファイル記憶手段と、

前記ファイル記憶手段に記憶された前記複数のファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、

表示装置と、

入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶された処理許可条件を読み出し、アクセスが認められているファイルを判別する許可判別手段と、

前記許可判別手段によりアクセスが認められていると判別されたファイルを、選択可能に前記表示装置に表示する表示制御手段と、

より構成されることを特徴とするコンピュータシステム。

【請求項11】複数のファイルを記憶するファイル記憶手段と、

前記ファイル記憶手段に記憶された複数のファイルのうち、所定の属性のファイルを表示する表示手段と、

前記ファイル記憶手段に記憶された前記複数のファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、

起動時に、前記ファイルの属性を一旦前記表示手段に表示されない属性に書き換える属性変更手段と、

外部より入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶されたアクセス許可条件を読み出し、アクセスが認められているファイルを判別する許可判別手段と、

前記許可判別手段により、アクセスが認められていると判別されたファイルを表示手段に表示可能な属性に変更する属性再変更手段と、

より構成されることを特徴とするコンピュータシステム。

【請求項12】ファイルを暗号状態で記憶するファイル記憶手段と、

前記ファイル記憶手段に記憶されたファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、

起動時に、外部より入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶されたアクセス許可条件を読み出し、アクセスが認められているか否かを判別する許可判別手段と、

前記許可判別手段により、アクセスが認められていると判別された場合に、前記ファイル記憶手段に記憶されたファイルの暗号化と復号化を行う手段と、

より構成されることを特徴とするコンピュータシステム。

【請求項13】前記操作者の身体的特徴を読み取って前記許可判別手段に供給する身体情報読取手段をさらに備え、

前記許可判別手段は、前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を含む、ことを特徴とする請求項5乃至12のいずれか1項に記載のコンピュータシステム。

【請求項14】前記コンピュータシステムの起動を認められた操作者の身体情報を保持する起動情報記憶手段と、

前記コンピュータシステムの起動時に取り込んだ身体情報と、前記起動情報記憶手段に登録された身体情報とを比較し、比較結果に基づいてこのコンピュータシステムの起動を継続または中断する手段を備える、

ことを特徴とする請求項1乃至13のいずれか1項に記載のコンピュータシステム。

【請求項15】前記身体情報は、指紋データ、網膜パターンのデータ、音声パターンのデータ、顔画像のデータのいずれかから構成され、

前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置のいずれかから構成される、

ことを特徴とする請求項1乃至4及び13のいずれか1項に記載のコンピュータシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コンピュータシステムに関し、特に、操作者から何らかの指示が入力された際に、その操作者がその指示を実行することが許容されているか否かを操作者の身体情報から判別し、指示された処理を実行又は拒否するコンピュータシステムに関する。

【0002】

【従来の技術】従来、コンピュータシステムの対話処理における機密保護のために、ユーザ（操作者）名及びパスワードをコンピュータシステムに予め登録することが行われていた。即ち、ユーザがログオンをしようとするときにユーザ名及びパスワードを入力させ、この入力されたユーザ名及びパスワードが予めコンピュータシステムに登録されたユーザ名及びパスワードと一致しない場合、そのユーザにログオンを認めないこととしていた。

【0003】また、従来の対話処理を行うコンピュータシステムでは、セッション中において、各ユーザから特定の処理を実行する旨の指示入力成された場合には、当該処理を実行するか否かを判断するため、予め、各ユーザにユーザID（Identifier）を割り当てて登録することが行われていた。即ち、ユーザからある処理を実行する旨の指示入力成された場合、当該指示入力したユーザに割り当てられたユーザIDによって、当該処理を実行するか否かをチェックしていた。

【0004】また、セッション中における各所の実行の許可をユーザIDによってチェックするのでは、セッション中にユーザが離席して他者が着席する可能性があるため、機密保護の万全を期し難かった。

【0005】

【発明が解決しようとする課題】しかし、ユーザ名及びパスワードによる機密保護では、各ユーザに、パスワードを他人が容易に推定出来ないように設定したり、パスワードを定期的に変更する等の負担が強いられていた。

【0006】この発明は上記実状に鑑みてなされたもので、ユーザに機密保護の負担をかけないコンピュータシステムを提供することを目的とする。また、セッション中にユーザが離席しても機密を保護することができるコンピュータシステムを提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、第1の発明に係るコンピュータシステムは、特定のユーザからの指示によってのみ開始する処理を実行するコンピュータシステムにおいて、ユーザの身体の一部の画像に基づくコード化画像データを記憶するとともに、当該ユーザからの指示によって前記処理を開始するか否かを示すデータを前記コード化画像データに対応させて記憶する記憶手段と、ユーザの身体の一部の画像を読み取る身体情報読取手段と、ユーザが前記指示を入力するための入力手段と、前記身体情報読取手段によって読み取られた前記画像に基づいて前記コード化画像データを生成し、当該コード化画像データに基づいて前記記憶手段を検索して当該コード化画像データに対応する前記データを読み込み、前記処理を開始する旨のデータを得た場合には前記処理を開始する制御手段と、を備えたことを特徴とする。

【0008】本願の第1の発明によれば、記憶手段によってユーザの指紋等の身体の一部の画像に基づくコード化画像データが記憶されると共に、当該ユーザからの指示によって前記処理を開始するか否かを示すデータが前記コード化画像データに対応させて記憶される。身体情報読取手段によって、ユーザの指紋の画像が読み取られる。入力手段によって、ユーザから前記指示が入力される。制御手段によって、前記身体情報読取手段によって読み取られた前記画像に基づいて前記コード化画像データが生成され、当該コード化画像データに基づいて前記記憶手段の検索がされ、当該コード化画像データに対応する前記データが読み込まれ、前記処理を開始する旨のデータが得られた場合には前記処理が開始される。

【0009】ここで、記憶手段とは、ハードディスク、光磁気ディスク等であり、身体情報読取手段とは、指紋読取装置であり、入力手段とは、キーボード、マウス等であり、制御手段とは、CPU (Central Processing Unit) 等である。

【0010】このように、ユーザの指紋の画像によつ

て、処理を開始するか否かが判断されるので、ユーザに機密保護のための負担が強いられることがない。

【0011】本願の第2の発明は、上述した目的を達成するため、前記データはビットデータであり、前記記憶手段は、前記コード化画像データ毎に前記ビットデータをワード化したデータを記憶することとしたものである。(請求項2に対応)

【0012】本願の第3の発明は、上述した目的を達成するため、前記処理に対して各々番号が付されており、前記ビットデータのビット番号が前記番号と同一であることを特定したものである。(請求項3に対応)

【0013】また、第4の発明は、前記制御手段は、前記指示の入力があったときに、前記番号を引数として受け取り、当該指示を入力したユーザの指紋の画像を読み取る旨を前記身体情報読取手段に対して指示し、前記身体情報読取手段によって読み取られた前記画像に基づいて前記コード化画像データを生成し、当該コード化画像データに基づいて前記記憶手段を検索し、検索結果が得られた場合には当該検索結果であるワードデータ中の前記番号をビット番号とするビットデータを抽出して戻り値とし、検索結果が得られなかった場合にはその旨を通知するデータを戻り値とするサブルーチンプログラムを実行することを特定したものである(請求項4に対応)。

【0014】第4の発明によれば、ユーザからの指示入力があったときに、ユーザの指紋画像を読み込むので、セッション中にユーザが離席して他者が着席している場合でも機密保護を図ることができる。

【0015】また、本願の第5の発明のコンピュータシステムは、特定の操作者からの指示によってのみ開始する処理、例えば、文書ファイルの開・閉、プログラムの実行等の処理を実行するコンピュータシステムにおいて、操作者の身体的特徴を示す身体情報を記憶するとともに、当該操作者からの指示によって前記処理を開始するか否かを示す処理許可条件を前記身体情報に対応させて記憶する記憶手段と、操作者が前記指示を入力するための指示入力手段と、前記指示入力手段からの所定の指示の入力に応答して、外部(例えば、外部に配置された指紋読み取り装置等から)から供給される操作者の身体情報を取り込む取込手段と、前記取込手段により取込まれた身体情報に基づいて前記処理許可条件を読み出し、前記指示入力手段により指示された処理を実行することが許可されているか否かを判別する許可判別手段と、を備えたことを特徴とする。(請求項5に対応)

【0016】この構成によれば、ユーザの身体的特徴の画像によって、処理を開始するか否かが判断されるので、ユーザに機密保護のための負担が強いられることがない。

【0017】また、本願の第6の発明のコンピュータシステムは、複数の処理について、操作者毎に処理を認め

るか否かを示す処理許可条件を記憶する許可条件記憶手段と、任意の処理を指示する指示入力手段と、前記指示入力手段により入力された指示に応答し、操作者の身体情報を入力し、該身体情報に基づいて前記許可条件記憶手段に記憶された処理許可条件を読み出し、前記指示入力手段により入力された処理を実行することが許可されているか否かを判別する許可判別手段と、前記許可判別手段が、認められていると判別した際に、前記指示入力手段により指示された処理を実行する処理手段と、より構成されることを特徴とする。(請求項6に対応)

【0018】この構成によっても、ユーザの身体情報によって、処理を開始するか否かが判断されるので、ユーザに機密保護のための負担が強いられることがない。

【0019】また、本願の第7の発明のコンピュータシステムは、請求項5又は6の発明において、前記指示入力手段は、入力操作を検出し、入力の内容を含む検出信号を出力する手段を含み、前記許可判別手段は、前記検出信号をフックするフック手段と、前記処理許可条件に従って、前記フック手段によりフックされた検出信号が指示する処理が、前記操作者に許可されているか否かを判別し、許可されていると判別した際に、前記検出信号を前記処理手段に供給する転送手段と、を含み、前記処理手段は、前記転送手段からの前記検出信号に従って前記指示入力手段により指示された処理を実行する手段を含む、ことを特徴とする。(請求項7に対応)

【0020】この構成によれば、検出信号をフックすることにより処理を開始するか否かを判断する。従って、検出信号を生成する手段及び処理を実行する手段は既存のものを使用することができ、システムの互換性を維持しつつ身体情報に基づいて処理の許可・不許可を自動的に判別し、ユーザに負担をかけることなく処理を制御することができる。

【0021】また、本願の第8の発明のコンピュータシステムは、所定のイベントの発生により開始され、操作者毎に処理を認めるか否かの別がある後続処理について、操作者毎に前記後続処理を認めるか否かを示す処理許可条件を記憶する許可条件記憶手段と、外部より入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶された処理許可条件を読み出し、前記後続処理を実行することが許可されているか否かを判別する許可判別手段と、前記許可判別手段が、認められていると判別した際に、前記後続処理を実行する後続処理実行手段とを含み、前記許可判別手段は、前記所定のイベントの発生を検出して前記許可判別手段に制御を移行させるイベント検出手段を含む、ことを特徴とする。(請求項8に対応)

【0022】この構成によれば、操作者の指示入力(10イベント)、プログラムの要求等の所定のイベントが発生すると、このイベントの発生が検出され、後続処理を認めるか否かが判断され、認められた場合に、後続処

理が実行される。従って、イベントを発生させる手段は既存のものを使用することができ、イベント検出手段と許可条件記憶手段及び許可判別手段を既存のシステムに追加するだけで、許可・不許可を自動的に判別し、処理を制御することができる。

【0023】また、本願の第9の発明のコンピュータシステムにおいて、前記後続処理は、ファイルの操作を含む処理、例えば、文書ファイルのファイルを開く、プログラムファイルを実行する(プログラムを実行する)等の処理から構成される。この場合、所定のイベントは、ファイルの操作を指示するイベント(例えば、操作者やアプリケーションプログラムによる所定のプログラムファイルの実行の指示、ファイルのオープン等の指示等)である。(請求項9に対応)

【0024】本願の第10の発明のコンピュータシステムは、複数のファイルを記憶するファイル記憶手段と、前記ファイル記憶手段に記憶された前記複数のファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、表示装置と、入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶された処理許可条件を読み出し、アクセスが認められているファイルを判別する許可判別手段と、前記許可判別手段によりアクセスが認められていると判別されたファイルを、選択可能に前記表示装置に表示する表示制御手段と、より構成されることを特徴とする。

【0025】この構成によれば、身体的情報に基づいて判別された操作者のアクセスが認められているファイルのみが、選択可能に表示装置に表示される。例えば、アクセスが認められているファイルのみがシンボル等で画面に表示され、アクセスが認められていないファイルは表示されない。或いは、アクセス可能なファイルが特定の選択可能なシンボル等で表示され、アクセスが認められていないファイルは他の選択できないシンボルで表示される。また、アクセス可能なファイルが選択可能なウインドウ内に表示され、アクセスが認められていないファイルは他の選択できないウインドウ内に表示される。このような構成によれば、身体情報に基づいてアクセスできるファイルをファイル及び操作者単位で制限することができ、ファイル単位・操作者単位での機密保持を図ることができる。

【0026】さらに、本願の第11の発明のコンピュータシステムは、複数のファイルを記憶するファイル記憶手段と、前記ファイル記憶手段に記憶された複数のファイルのうち、所定の属性のファイルを表示する表示手段と、前記ファイル記憶手段に記憶された複数のファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、起動時に、前記ファイルの属性を一旦前記表示手段に表示されない属性に書き換える属性変更手段と、外部

より入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶されたアクセス許可条件を読み出し、アクセスが認められているファイルを判別する許可判別手段と、前記許可判別手段により、アクセスが認められていると判別されたファイルを表示手段に表示可能な属性に変更する属性再変更手段と、より構成されることを特徴とする。(請求項11に対応)

【0027】この発明によれば、身体情報に基づいて、アクセスが認められているファイルのみが表示され、アクセスが認められていないファイルは表示されない。従って、ファイル単位及び操作者単位で機密を保持することができる。

【0028】さらに、本願の第12の発明のコンピュータシステムは、ファイルを暗号状態(圧縮状態を含む)で記憶するファイル記憶手段と、前記ファイル記憶手段に記憶されたファイルについて、操作者毎にファイルへのアクセスを認めるか否かを示すアクセス許可条件を記憶する許可条件記憶手段と、起動時に、外部より入力された操作者の身体情報に基づいて、前記許可条件記憶手段に記憶されたアクセス許可条件を読み出し、アクセスが認められているか否かを判別する許可判別手段と、前記許可判別手段により、アクセスが認められていると判別された場合に、前記ファイル記憶手段に記憶されたファイルの暗号化(圧縮を含む)と復号化(伸張を含む)を行う手段と、より構成される。

【0029】この構成によれば、身体情報に基づいて、アクセスの権限があると認められた場合のみ、ファイルの暗号化と復号の少なくとも一方が実行される。従って、例えば、復号ができない場合には、権限なき者はファイルを開いたり、実行すること自体ができない。また、暗号化ができない場合は、元の暗号化されたファイルを更新することができない。従って、ユーザ単位・ファイル単位、さらに、アクセスの種類単位でデータの機密を保持することができる。

【0030】また、本願の第13の発明のコンピュータシステムは、第5～第12の発明において、操作者の身体的特徴を読み取る身体情報読取手段をさらに備え、前記許可判別手段は、前記身体情報読取手段による身体情報の入力を促すメッセージを表示する手段を含む、ことを特徴とする。(請求項13に対応)

この構成によれば、割り込みの要求が発生した場合等のユーザの確認が必要になった際に、メッセージを表示して身体情報の入力を促すことができる。

【0031】さらに、前記コンピュータシステムの起動を認められた操作者の身体情報を保持する起動情報記憶手段と、前記コンピュータシステムの起動時に、取り込んだ身体情報と、前記起動情報記憶手段に登録された身体情報とを比較し、比較結果に基づいてこのコンピュータシステムの起動を継続または中断する手段を配置しても良い。

【0032】このような構成とすることにより、コンピュータのログイン自体を身体情報に基づいて制御できる。

【0033】前記身体情報は、例えば、指紋データ、網膜パターンデータ、音声パターンデータ、顔画像データのいずれかから構成される。この場合、前記身体情報読取手段は、指紋読取装置、網膜パターン読取装置、音声パターン読取装置、顔画像読取装置のいずれかからなる。

10 【0034】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

(第1の実施の形態)図1～図5を参照して、この発明の第1の実施の形態に係るコンピュータシステムを説明する。

【0035】図1は、第1の実施の形態によるコンピュータシステムの構成を示したブロック図である。図1において、コンピュータシステムは、バスBによって相互に接続された指紋読取装置1と、キーボード2と、表示装置3と、外部記憶装置4と、画像メモリ5と、汎用メモリ6と、制御部7とから構成されている。

【0036】指紋読取装置1は、人間の指紋の画像を読み取って、その画像データをバスBへ伝達するための装置である。この指紋読取装置1が、身体情報読取手段に相当する。

【0037】キーボード2は、ユーザが文字等のデータを入力するための入力装置である。このキーボード2が入力手段に相当する。

【0038】表示装置3は、キーボード2から入力されたデータ等を表示するCRTである。尚、この表示装置3は、液晶ディスプレイであっても良い。

【0039】外部記憶装置4は、制御部7が処理するプログラムや、ユーザマスタファイル等を記憶するハードディスク装置である。この外部記憶装置4が、記憶手段及び媒体に相当する。

【0040】ここで、ユーザマスタファイルは、各ユーザの指紋の画像データを一定のアルゴリズムに従ってコード化した指紋コードと、各指紋コードに対応させたアクセス許可データとにより、構成されている。このアクセス許可データは、この実施の形態のコンピュータシステム上で実行されるアプリケーションプログラム中において、特定のユーザに対してのみ事項が許可されている処理(例えば、データベースの更新処理等)(以下「認証ポイント」という)の総数と同数のビットデータからなるものである。これらの認証ポイントの各々には、一対一に対応付けられた番号(以下「認証ポイント番号」という。)が付与されている。

【0041】アクセス許可データ中の各ビットデータと各認証ポイントとは、当該ビットデータのビット番号と当該認証ポイントの認証ポイント番号とが一致するよう

に、対応付けられている。このアクセス許可データ中の各ビットデータの内容が、当該アクセス許可データが対応づけられた指紋コードの基となった指紋を有するユーザに対して当該ビットデータが対応づけられた認証ポイントの実行が許可されているか否かを示している。即ち、アクセス許可データ中のあるビットデータが1であることは、当該アクセス許可データが対応づけられたユーザに対して当該ビットデータに対応づけられた認証ポイントの実行が許可されていることを示している。また、アクセス許可データ中のあるビットデータが0であることは、当該アクセス許可データが対応づけられたユーザに対して、当該ビットデータに対応づけられた認証ポイントの実行が許可されていないことを示している。

【0042】アクセス許可データを図2を参照して説明する。図2は、アクセス許可データの例を示した概念図である。図2において、このアクセス許可データ10は、8ビットのビットデータから構成されている。即ち、図2に示されるアクセス許可データ10において、ビット番号0のビットデータ”1”は、アクセス許可データ10が対応づけられた指紋コードの基となる指紋を有するユーザに対して認証ポイント番号0の認証ポイントの実行が許可されていることを示している。また、ビット番号1のビットデータ”0”は、アクセス許可データ10が対応づけられた指紋コードの基となる指紋を有するユーザに対して認証ポイント番号1の認証ポイントの実行が許可されていないことを示している。

【0043】画像メモリ5は、RAM(Random Access Memory)等で構成され、指紋読取装置1によって読み取られた指紋の画像データを保持するためのメモリである。

【0044】汎用メモリ6は、RAM等で構成され、制御部7が作業用に使用するためのメモリである。制御部7は、CPU(Central Processing Unit)等で構成され、指紋読取装置1、表示装置3、外部記憶装置4に対して、それぞれ指紋読み取り指示、画像表示指示、データ書き込みもしくは読み込み指示を行う。また、制御部7は、指紋読取装置1によって読み取られた指紋の画像データの処理、キーボード2から入力された文字等のデータの処理、表示装置3に表示する画面データの処理、外部記憶装置4からのデータの読み込み処理、外部記憶装置4へのデータの書き込み処理を行う。この制御部7が、制御手段に相当する。

【0045】図3は、このコンピュータシステムの主要部の論理構造を示す。図示するように、このコンピュータシステムはアプリケーションプログラム11と、個人認証用の指紋読取装置1を駆動するデバイスドライバ12とから構成される。

【0046】アプリケーションプログラム11は、必要に応じてデバイスドライバ12に個人認証を要求し、デバイスドライバ12から認証結果を受け取り、データ処

理にこの認証結果を利用する。デバイスドライバ12は、例えば、アプリケーションプログラム11のサブルーチンとして構成され、アプリケーションプログラム11の要求に応じて、指紋読取装置1に指紋の読み取りを要求する命令を送信する。さらに、デバイスドライバ12は、指紋読取装置1から指紋の画像データを受信し、これをコード化し、このコードデータをキーとしてユーザマスタファイルを検索して、個人認証を行い、認証結果をアプリケーションプログラムに引き渡す。

10 【0047】<第1の実施の形態の動作の説明>次に、本発明の実施の形態の動作について、図4及び図5のフローチャートを参照して説明する。図4のフローチャートは、この実施の形態のコンピュータシステムにおけるデータベース更新処理プログラムを示している。このデータベース更新処理は、特定のユーザのみ開始が認められた処理であり、上述した認証ポイントに相当する処理である。また、図5のフローチャートは、ユーザ認証のためのサブルーチンプログラム(デバイスドライバ12)の動作を示している。このサブルーチンプログラムは、本実施の形態のコンピュータシステム上のアプリケーションプログラム中における各認証ポイントの実行に際して読み出されるものである。

【0048】図4のフローチャートにおいて、制御部7は、まず、ユーザからデータベース更新処理開始指示が成された旨のデータがキーボード2から通知されるのを待つ(S001)。

【0049】データベース更新処理開始指示の通知が来たら、制御部7は、本更新処理に付与された認証ポイント番号のデータを引数として、図5に示すユーザ認証サブルーチン処理を行う(S002)。

【0050】図5に示すユーザ認証サブルーチン処理を開始すると、制御部7は、まず、ユーザの指紋を読み取るように指紋読取装置1に対して指示する(S101)。そして、制御部7は、ユーザの指紋の画像データを指紋読取装置1から受信するのを待つ(S102)。

【0051】ユーザの指紋の画像データを指紋読取装置1から受信したら、制御部7は、受信した指紋の画像データを一定のアルゴリズムに従ってコード化し、指紋コードを得る(S103)。

40 【0052】そして、制御部7は、ステップS103で得た指紋コードをキーとして、外部記憶装置4に記憶されたユーザマスタファイルを検索する(S104)。そして、制御部7は、当該指紋コードに対応付けられたアクセス許可データが得られたら処理をS106へ移し、アクセス許可データが得られなければ処理をS108へ移す(S105)。

【0053】S106において、制御部7は、S104で得たアクセス許可データの中から、引数として受け取った認証ポイント番号に対応するビットデータを抽出する。そして、この抽出したビットデータの値を戻り値と

して (S107)、ユーザ認証サブルーチン処理を終了する。

【0054】一方、S105において、アクセス許可データが得られなかった場合、即ち、ユーザマスタファイルに当該ユーザの指紋コードが登録されていない場合は、-1を戻り値として (S108)、ユーザ認証サブルーチン処理を終了する。

【0055】制御部7は、ユーザ認証サブルーチンの処理を終了すると、データベース更新処理プログラムの処理をS003から再開する。S003において、制御部7は、ユーザ認証サブルーチンからの戻り値が-1であるか否かをチェックする。そして、戻り値が-1であれば、処理をS004に移し、そうでなければ、処理をS005に移す。

【0056】戻り値が-1であった場合、制御部7は、データベース更新処理開始指示をしたユーザがユーザ登録されていないユーザである旨のメッセージを表示装置3に表示する (S004)。そして、その後、処理を終了する。

【0057】一方、S003において、戻り値が-1でなかった場合、制御部7は、さらに、戻り値が0であるか否かをチェックする。戻り値が0であれば、処理をS006へ移し、そうでなければ処理をS007に移す (S005)。

【0058】S006において、制御部7は、データベース更新処理開始指示をしたユーザがデータベース更新処理を行うことが認められていないユーザである旨のメッセージを表示装置3に表示する。その後、処理を終了する。

【0059】一方、S005において戻り値が0でなかった場合、制御部7はデータベースを更新するためのデータが入力されるのを待つ (S007)。更新するためのデータが入力されたら、制御部7は、当該データに基づいてデータベースを更新する (S008)。そして、その後処理を終了する。

【0060】以上説明したように、この実施の形態によれば、ユーザに負担をかけることなく、機密保持を図ることができる。また、各認証ポイントの実行に際してユーザの認証を行うので、セッション中にユーザが離席しても、機密を保護することができる。さらに、コンピュータシステムにユーザ登録されていないユーザを検出することもできる。

【0061】なお、以上の説明では、データベースにアクセスする場合に、アクセスを認めるか否かを指紋を用いて判別したが、この発明は個人認証が必要な任意の場合にも適用可能である。即ち、任意のアプリケーションプログラムに上述の個人認証ステップを組み込むことにより、使用者別に特定のファイルの読み込み・書き込みの許可・禁止、特定のファイルグループの読み込み・書き込みの許可・禁止、共通利用者用に読み出し・書き込

み可能なファイルグループの指定等に使用することができる。

【0062】なお、コンピュータ本体と指紋読取装置1との間のデータ通信を、図6に示すように、暗号化することも可能である。この場合、デバイスドライバ12は、指紋読取装置1に認証要求の命令を送信する際、指紋読取装置1に依存する手順を使用し、また、認証要求の命令を暗号化する。一方、指紋読取装置1は、コンピュータ本体からの命令を復号して要求を認識し、ユーザの指紋を読み取って、これを暗号化してデバイスドライバ12に送信する。デバイスドライバ12は、指紋読取装置1からの指紋の画像データを受信し、これを復号し、さらにコード化する。その後、ユーザマスタファイルを検索して戻り値を求め、アプリケーションプログラム11に戻り値 (認証結果) を引き渡す。

【0063】(第2の実施の形態) 第1の実施の形態においては、1つのアプリケーションプログラム内で特定の処理を認めるか否かを判別するための個人認証に指紋データを使用したのが、例えば、ファイルのアクセスを認めるか否かを判断するための個人認証に指紋データを使用することも可能である。このような処理を行う第2の実施の形態を以下に説明する。

【0064】この実施の形態のコンピュータシステムの物理的構成は基本的に図1に示す構成と同一である。一方、この実施の形態のコンピュータシステムは、論理的には、図7に示すように、OS (オペレーティングシステム) 21と、ファイル制御プログラム31とから構成されている。

【0065】OS (オペレーティングシステム) 21は、キーボード2の入力操作を検出する入力部22と、入力部22により検出された入力指示に従った処理を実行する処理部24と、表示装置3を制御する表示制御部23を備える。処理部24は、ファイルをアクセスするためのファイル処理部25を含む。

【0066】一方、ファイル制御プログラム31は、イベントが発生したことを検出し、そのイベントがファイル操作に関するものである場合に、そのファイル操作を許可するか拒否するかを制御するためのプログラムである。図7は、OS21が、DOS (ディスクオペレーティングシステム) であるとした場合の例であり、ファイル制御プログラム31は、入力フック部32と、ドライバ部33と、ユーザマスタファイル39とから構成される。入力フック部32は、割り込み要求が発行された (イベントの発生) とき、ファイル制御プログラム31が存在しないときに行われるべき処理を行わず、該処理に先立ちドライバ部33に処理を行わせる (フックする)。ユーザマスタファイル39は、図8に示すように、ユーザ毎、即ち、指紋データ毎に操作できるファイルのリストからなる。なお、このユーザマスタファイル39自体は、このコンピュータシステムの管理者のみが

アクセスできるように設定されている。

【0067】ドライバ部33は、処理内容判別部34と、メッセージ表示部35と、コード化部36と、判別部37と、送信部38とから構成される。

【0068】処理内容判別部34は、入力フック部32により取り込まれた入力情報を解析し、その内容がファイルの操作を指示しているか否かを判別し、指示している場合には、コード化部36に指紋の読み取りを指示すると共に判別部37に入力情報を提供する。また、フックされた入力情報がファイルの操作を指示していない場合

には、検出信号を送信部38に送る。  
【0069】メッセージ表示部35は、処理内容判別部34が「入力ファイルの操作を指示している」と判別した場合に、指紋情報の入力を促す画面をOS21の表示制御部23を介して表示装置3に表示する。また、判別部37が「要求されたファイル操作がそのユーザに認められていない」と判断した際に、アクセスが拒否されたことを示す画面を表示制御部23を介して表示装置3に表示する。

【0070】コード化部36は、処理内容判別部34からの指示に従って指紋読取装置1に指紋の読み取りを指示し、また、指紋読取装置1から指紋の画像を取り込み、これをコード化し、コード化指紋データを生成する。判別部37は、コード化部36で生成されたコード化指紋データに基づいて、ユーザマスタファイル39を参照し、そのコード化指紋データを有する者が該当ファイルをアクセスする権限を有するか否かを判別する。そして、権限を有すると判断した場合には、送信部38にアクセスを許可する信号とフックした検出信号を送信する。また、権限を有していないと判別した場合には、メ

ッセージ表示部35にアクセスを許可しない旨のメッセージを表示させる。

【0071】＜第2の実施の形態の動作＞第2の実施の形態のコンピュータシステムの動作を図9及び図10のフローチャートを参照して説明する。  
【0072】OS21が予めインストールされたコンピュータにファイル制御プログラム31をインストールする際、ファイル制御プログラムインストーラ（図示せず）は、OS21の起動後、ファイル制御プログラム31が自動的に起動するようにシステムを設定する。

【0073】次に、このコンピュータシステムの通常動作時の動作を図9を参照して説明する。まず、電源が投入されると、OS21が起動する（S201）。次に、ファイル制御プログラム31が起動する（S202）。ファイル制御プログラム31の入力フック部32は、起動すると、OS21の入力部22が発生する割り込み要求に対応する処理のアドレスを、処理部24からドライバ部33のアドレスに書き換える（S203）。

【0074】例えば、OS21がマイクロソフト社から提供されているMS-DOS（登録商標）の場合には、

主メモリとして機能する汎用メモリ6上に作成される割り込みテーブル中、入力に関するシステムコールの割込INT21に対応する処理のアドレスをドライバ部33のアドレスとする。以上で、起動時の設定動作は終了する。

【0075】この状態で、キーボード2から何らかの入力があると、OS21の入力部22は、この入力操作を判別し、必要に応じて割り込み要求を発する（IOイベントの発生）。この割り込み要求に対応する処理は、通常は、処理部24で行うが、ファイル制御プログラム31の起動時にドライバ部33のアドレスに書き換えられている。従って、処理はドライバ部33に移行され、フックされる（図10S301）。

【0076】処理内容判別部34は、OS21から入力された検出信号を解析し（S302）、入力内容がファイルの操作（ファイルを開く、実行ファイルを起動する等）を指示しているか否かを判別する（S303）。入力内容がファイルの操作を指示している場合には、コード化部36を介して指紋読取装置1に指紋の読み取りを指示する（S304）。さらに、メッセージ表示部35に指紋の入力を促すメッセージの表示を指示する。メッセージ表示部35は、処理内容判別部34の指示に従い、OS21の表示制御部23を介して表示装置3に、指紋の入力を促すメッセージを表示する（S305）。コード化部36は、指紋読取装置1からの指紋の画像データの入力を待機し（S306）、画像データが入力されると、この画像データをコード化指紋データに変換し、判別部37に提供する（S307）。

【0077】判別部37は、ユーザマスタファイル39を参照し、コード化部から供給されたコード化指紋データを有する者が、入力操作で指示されたファイルの操作を認められているか否かを判別する（S308）。判別部37は、アクセスが認められていると判断すると、送信部38に検出信号を供給する。送信部38は処理をOS21の処理部24に引き渡す（S309）。処理を引き渡された処理部24は指示されたファイルを処理する。

【0078】一方、ステップS308で、判別部37によりファイル操作が認められていないと判断された場合、メッセージ表示部35は、OS21の表示制御部23を介して表示装置3に「アクセスが許可されていません」等のファイル操作を拒否するメッセージを表示する（S310）。

【0079】ステップS303で、処理内容判別部34が指示内容がファイルの操作ではないと判断した場合には、送信部38によりOS21の処理部24に処理が引き渡される（S311）。処理部24は、指示に対応する処理を行う。

【0080】システムがシャットダウンされる際には、ファイル制御プログラム31は、OS21の入力部22

が発生する割り込み要求に対応する処理のアドレスを通常のアドレスに書き換えてから終了する。

【0081】このような構成によれば、例えば、デスクトップ上で任意のプログラムの起動を指示した場合には、この指示が入力フック部32でフックされ、判別部37でアクセスを許可するか否かがユーザマスタファイル39に従って判別され、許可の場合のみそのプログラムが起動される。

【0082】また、アプリケーションプログラム、例えば、ワードプロセッサ等を起動した後で、任意の文書ファイルを開くような場合にも、指示操作が入力フック部32でフックされ、判別部37でアクセスを許可するか否かが判別され、許可の場合のみそのファイルが開かれる。

【0083】以上説明したように、この第2の実施の形態によれば、ファイル制御プログラム31が、入力指示を自動的に取り込んで、指示されたファイルをアクセスする権限を有するか否かをコード化指紋データに基づいて判別し、権限を有する場合にはそのファイルのアクセスを許可する。従って、ユーザに負担をかけることなくコンピュータの機密保持を実行することができる。

【0084】また、ファイル制御プログラム31をインストールするだけでファイル操作を制御することができ、既存のOS、アプリケーションプログラム等に修正を加える必要がなく、そのまま使用することができる。

【0085】なお、以上の説明では、起動時にファイル制御プログラム31が、入力部22の割り込み要求に対応する処理のアドレスを書き換えたが、ファイル制御プログラム31のインストール時に割り込み要求に対応する処理のアドレスを書き換え、アンインストール時に元のアドレスに書き換えてもよい。

【0086】以上の説明では、ファイルのアクセスの可否を指紋データに基づいて判別したが、任意の指示（例えば、特定のデータの表示、ポートへの出力）の入力について指紋データに基づいて、指示された処理の実行を認めるか否かを判別してもよい。また、入力指示もキーボード2によるものに限定されず、マウス、トラックボール、タブレット等、任意の入力装置を使用することができる。

【0087】また、アプリケーションプログラムが、そのプログラムの必要によりファイルをアクセスする場合等にOS21で発生する割り込みの要求（イベント）をファイル制御プログラム31でフックして、その内容を判別し、指紋の入力を要求すると共に指紋読取装置1から入力された指紋データに基づいてそのファイルへのアクセスを認めるか否かを判別してもよい。

【0088】また、ユーザのアクセスを認めるか否かをコード化指紋データに基づいて判別したが、第1の実施の形態と同様に、引数を用いてユーザとして登録されているか否か、登録されている場合には指示したファイル

へのアクセスが認められているか否か等を判別してもよい。

【0089】OS21は、DOSに限定されず、いわゆる、ウィンドウシステム、unix等、任意のものを使用することができる。これらのOSを使用する場合には、各OSのプロパティに応じて、適宜ファイルへのアクセス或いは割り込みの要求、リンクの発生等の所定のイベントを検出し、指紋データの入力を促すと共に操作者がファイルをアクセスする権限を有するか否かを判別すればよい。

【0090】（第3の実施の形態）第2の実施の形態においては、入力操作が行われる度に、ファイル操作の可否を判別したが、各ユーザに、そのユーザが操作できるファイルのみを表示するようにしてもよい。このような処理を行う第3の実施の形態を以下に説明する。

【0091】この実施の形態のコンピュータシステムの物理的構成は基本的に図1に示す構成と同一である。ただし、外部記憶装置4には、図12を参照して詳述するファイル制御プログラムと、図8に示すユーザマスタファイルとが記憶されている。

【0092】図11は、この実施の形態のコンピュータシステムの論理構成を示す。図示するように、このコンピュータシステムは、論理的に、OS（オペレーティングシステム）21と、属性制御プログラム51と、ユーザマスタファイル（アクセス許可テーブル）39とから構成されている。属性制御プログラム51は、属性制御プログラムインストーラ（図示せず）によって、OS21が予めインストールされたコンピュータにインストールされるが、その際、該属性制御プログラムインストーラは、OS21の起動後、属性制御プログラム51が自動的に起動するようにシステムを設定する。

【0093】属性制御プログラム51は、OS21の起動に伴って起動され、ファイルの属性を一旦隠しファイルに変更する機能と、コード化指紋データとユーザマスタファイル39とを照合してアクセスが認められるファイルを判別し、これらのファイルを元の属性に戻す機能を有する。

【0094】次に、このコンピュータシステムの起動時の動作を図12のフローチャートを参照して説明する。

まず、コンピュータシステムの電源が投入されると、OS21が起動され（S401）、続いて、属性制御プログラム51が起動される（S402）。属性制御プログラム51は、起動されると、OS21を介して外部記憶装置4を検索し、外部記憶装置4に格納されている全てのファイルの元の属性をセーブすると共にこれらのファイルの属性を変更し、OS21が表示装置3に表示しない属性、いわゆる隠しファイルに変更する（S403）。

【0095】続いて、属性制御プログラム51は、指紋を入力すべき旨のメッセージをOS21を介して表示装

10

20

30

40

50

置 3 に表示し (S 4 0 4)、指紋読取装置 1 に指紋の読み取りを指示する (S 4 0 5)。メッセージに従って、ユーザが指紋読取装置 1 から指紋を入力すると (S 4 0 6)、属性制御プログラム 5 1 は、指紋読取装置 1 から入力された指紋の画像データをコード化指紋データに変換し、これをユーザマスタファイル 3 9 と照合し、そのユーザのアクセスが認められているファイルを判別する (S 4 0 7)。

【0096】次に、セーブしておいたファイル属性に基づいて、ユーザにアクセスが認められているファイルの属性を元に戻す (S 4 0 8)。以後の、通常の処理に移る。

【0097】また、システムのシャットダウン時には、属性制御プログラム 5 1 により外部記憶装置 4 に格納されているファイルの属性を元の属性に戻した後、属性制御プログラム 5 1 を閉じ、続いて、OS 2 1 を閉じる。

【0098】このような構成によれば、ユーザは自己のアクセスが認められているファイルのみを認識できる。従って、ファイルのアクセスを指紋に基づいて制御することができる。

【0099】以上の説明では、アクセスが認められているファイルのみを表示装置 3 に表示したが、アクセスが認められているファイルのみを選択可能とするならば表示方法及び選択手法は任意である。例えば、入力された指紋に基づいてアクセスが認められているファイルと認められていないファイルを判別し、アクセスが認められているファイルのみをカーソルがその中に移動可能なウインドウ内に表示し、アクセスが認められていないファイルをカーソルがその中に移動できないウインドウ内に表示してもよい。また、アクセスが認められているファイルのみを選択可能なシンボルで表示し、認められていないファイルを選択できないシンボルで表示してもよい。

【0100】(第 4 の実施の形態) 次に、この発明の第 4 の実施の形態のコンピュータシステムを説明する。この実施の形態のコンピュータシステムの物理的構成は基本的に図 1 に示す構成と同一である。ただし、外部記憶装置 4 の記憶データは圧縮 (または暗号化) されている。この圧縮データには、このコンピュータシステムを使用することを認められたユーザの個人認証データも含まれている。一方、論理的には、図 1 3 に示すように、OS 2 1 と OS 2 1 上で動作し、指紋読取装置 1 で読み取った指紋データに基づいて外部記憶装置 4 に格納されている圧縮データを処理する制御プログラム 6 1 からなる。制御プログラム 6 1 は、圧縮制御プログラムインストーラ (図示せず) によって、OS 2 1 が予めインストールされたコンピュータにインストールされるが、その際、該圧縮制御プログラムインストーラは、OS 2 1 の起動後、制御プログラム 6 1 が自動的に起動するようにシステムを設定する。

【0101】次に、この実施の形態のコンピュータシステムの動作を図 1 4 のフローチャートを参照して説明する。このコンピュータシステムが起動されると、まず、OS 2 1 が起動し (S 5 0 1)、続いて、制御プログラム 6 1 が起動する (S 5 0 2)。制御プログラム 6 1 は、外部記憶装置 4 の所定の領域をアクセスし、このシステムを使用することが許可されているユーザの個人認証データを読み出す (S 5 0 3)。

【0102】次に、制御プログラム 6 1 は、ユーザに指紋を入力すべき旨のメッセージを表示する (S 5 0 4)。さらに、指紋読取装置 1 に指紋の読み取りを指示する (S 5 0 5)。ユーザはこの表示に従って指紋入力装置 1 から指紋を入力する (S 5 0 6)。制御プログラム 6 1 は入力された指紋の画像データをコード化し (S 5 0 7)、ステップ S 5 0 3 で読み出された個人認証データとコード化指紋データとを照合し (S 5 0 8)、一致するものがあるか否かを判別する (S 5 0 9)。一致するものがある場合には、そのユーザがこのコンピュータシステムを使用することが認められていると判断し、主メモリに制御プログラム 6 1 を常駐させる (S 5 1 0)。

【0103】一方、指紋読取装置 1 から読み取った指紋の画像データがアクセス許可データに含まれている指紋データのいずれとも一致しないと判断した場合 (S 5 0 9)、そのユーザがこのコンピュータシステムを使用することが認められていないと判断し、主メモリに制御プログラム 6 1 の常駐を中止する (S 5 1 1)。以後は、通常の動作に移行する。

【0104】このような構成によれば、コンピュータの使用が認められている者の利用時は、制御プログラム 6 1 が主メモリに常駐する。従って、図 1 5 に示すように、外部記憶装置 4 に格納されている各種データを制御プログラム 6 1 で復元して通常のデータとして読み出して、アプリケーションプログラムで処理することができる。また、アプリケーションプログラムで作成・加工したデータを通常の方法で保存すると、制御プログラム 6 1 がこれを圧縮して外部記憶装置 4 に格納する。一方、ユーザが非登録者の場合には、制御プログラム 6 1 が主メモリに常駐しない。従って、外部記憶装置 4 に格納されているプログラム及び各種データを復元することができない。従って、このシステム自体を使用すること自体が困難となる。

【0105】なお、以上の説明では、外部記憶装置 4 全体を 1 種類の圧縮方法で圧縮したが、外部記憶装置 4 を図 1 6 に示すように、複数の領域に分割し、各領域をそれぞれ異なった圧縮方法で圧縮することも可能である。図 1 6 では、複数の領域に共通の共通領域に制御データ、OS 等が記録される。さらに、この共通領域には、このコンピュータシステムの使用が許可されているユーザのコード化指紋データと使用が許可されている記憶領

域が対応付けて記憶されている。

【0106】このような構成のコンピュータシステムの動作も、基本的には図14のフローチャートに示す動作と同一である。即ち、コンピュータシステムが起動されると、まず、OSが起動し（S501）、続いて、制御プログラム61が起動する（S502）。制御プログラム61は、外部記憶装置4の共通領域をアクセスし、この共通領域に格納されている認証データを読み出す（S503）。

【0107】次に、制御プログラム61は、ユーザに指紋を入力すべき旨のメッセージを表示し（S504）、指紋読取装置1に指紋の読み取りを指示する（S505）。指紋入力装置1が指紋を入力すると（S506）、制御プログラム61は入力された指紋の画像データをコード化する（S507）。さらに、このコード化画像データと認証データとを照合し（S508）、一致するものがあるか否かを判別する（S509）。一致するものがある場合には、主メモリに対応する領域用の制御プログラム61を常駐させる（S510）。

【0108】一方、指紋読取装置1から読み取った画像データのコード化データが認証データと一致しないと判断した場合には、そのユーザがこのコンピュータシステムを使用することが認められていないと判断し、主メモリに制御プログラム61の常駐を中止する（S511）。以後は、通常の動作に移行する。

【0109】このような構成によれば、ユーザが使用者として登録されている場合は、そのユーザが利用可能な領域の圧縮方法に対応する制御プログラム61が主メモリに常駐し、データの圧縮・復元を可能とする。従って、外部記憶装置4の使用領域を使用者別に分けて使用することができ、しかも、機密を保持することができる。

【0110】（第5の実施の形態）以上の実施の形態では、指紋に基づいた個人認証により、アプリケーションプログラム、ファイル等を制御する場合を説明したが、例えば、指紋による個人認証によりOSの起動、コンピュータのログインを制御することも可能である。

【0111】この場合、例えば、図17及び図18に示すように、OSの起動の途中で、パスワードによる個人認証を行う代わりに、指紋の入力を促すメッセージを表示し（S601）、さらに、指紋読取装置1に指紋の読み取りを指示する（S602）。指紋が入力されると（S603）、入力された指紋の画像をコード化し（S604）、予め登録されていた使用許可者のコード化指紋データと照合し（S605、S606）、一致した場合に起動処理を続行し（S607）、不一致の場合に起動処理を中断し、システムをシャットダウンする（S608）。このような構成によれば、指紋による個人認証により、OSの起動を制御することができ、コンピュータのログイン、ネットワーク接続時にログイン等を制御

することができる。

【0112】また、第1～第5の実施の形態の各認証システムを組み合わせることも可能である。例えば、コンピュータのログイン時に指紋による個人認証を行い、さらに、そのユーザのアクセスが認められているファイルのみを表示し、さらに、各ファイルへのアクセスが指示される度に指紋による認証を行ってもよい。

【0113】なお、指紋読取装置1とコンピュータ本体とはネットワーク等で接続されてもよい。

【0114】以上の実施の形態では、認証のために、コード化指紋データを使用した。指紋データの種類の任意である。例えば、指紋の画像データをフーリエ変換し、その位相情報を抽出し、これを指紋データとして使用することも可能である。この場合は、予め登録しておいた位相情報と指紋読取装置で読み取った画像から抽出した位相情報の相関度等を比較し、相関度が一定レベル以上の場合に、2つの指紋が一致すると判断する。

【0115】以上の実施の形態では、個人認証のために、指紋を使用した。網膜の血管パターン、音声パターン、顔の画像等を認証情報として使用することも可能である。

【0116】なお、この発明のコンピュータは、専用のシステムによらず、通常の指紋読取装置等と通常のコンピュータシステムを用いて実現可能である。例えば、指紋読取装置を接続したコンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、CD-ROM等）から該プログラムをインストールすることにより、上述の処理を実行するコンピュータシステムを構成することができる。

【0117】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でも良い。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0118】

【発明の効果】以上説明したように、この発明によれば、ユーザの身体情報に基づいて、ユーザにほとんど負担をかけることなく、機密を保持することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態によるコンピュータシステムの物理的構成を示すブロック図

【図2】アクセス許可データの例を示した概念図

【図3】本発明の第1の実施の形態によるコンピュータシステムの論理的構成を示す図

【図4】図1の制御部において実行される制御処理を示すフローチャート

【図 5】図 1 の制御部において実行される制御処理を示すフローチャート

【図 6】本発明の第 1 の実施の形態によるコンピュータシステムの変形例の論理的構成を示す図

【図 7】本発明の第 2 の実施の形態によるコンピュータシステムの物理的構成を示すブロック図

【図 8】ユーザマスタファイルの例を示した図

【図 9】第 2 の実施の形態のコンピュータシステムの起動時の処理を示すフローチャート

【図 10】第 2 の実施の形態のコンピュータシステムの 10 入力操作時の処理を示すフローチャート

【図 11】本発明の第 3 の実施の形態によるコンピュータシステムの論理的構成を示すブロック図

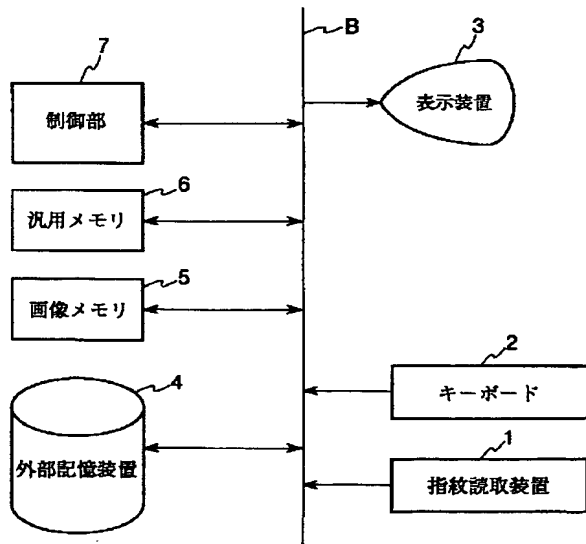
【図 12】第 3 の実施の形態のコンピュータシステムの起動時の処理を示すフローチャート

【図 13】本発明の第 4 の実施の形態によるコンピュータシステムの論理的構成を示すブロック図

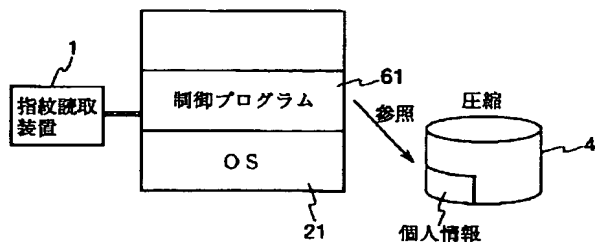
【図 14】第 4 の実施の形態のコンピュータシステムの起動時の処理を示すフローチャート

【図 15】制御プログラムによるデータ処理の様子を示す 20

【図 1】



【図 13】



図

【図 16】本発明の第 4 の実施の形態によるコンピュータシステムの変形例の外部記憶装置の論理的構成を示すブロック図

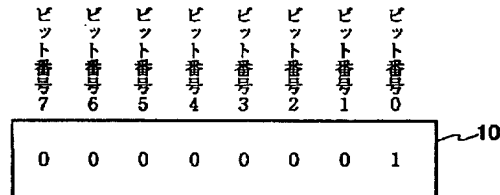
【図 17】第 5 の実施の形態のコンピュータシステムの論理的構成を示す図

【図 18】第 5 の実施の形態のコンピュータシステムの起動時の処理を示すフローチャート

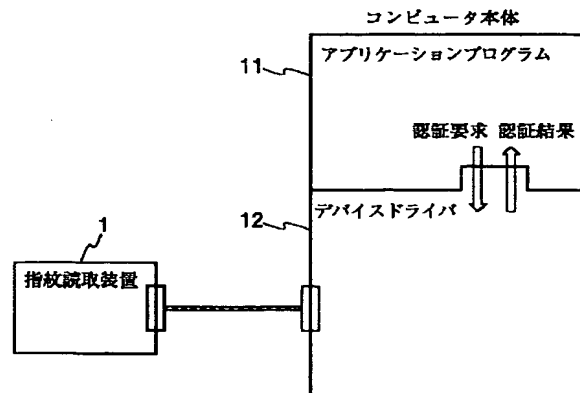
【符号の説明】

- 1 指紋読取装置
- 2 キーボード
- 3 表示装置
- 4 外部記憶装置
- 5 画像メモリ
- 6 汎用メモリ
- 7 制御部
- 10 アクセス許可データ
- 11 アプリケーションプログラム
- 12 デバイスドライバ

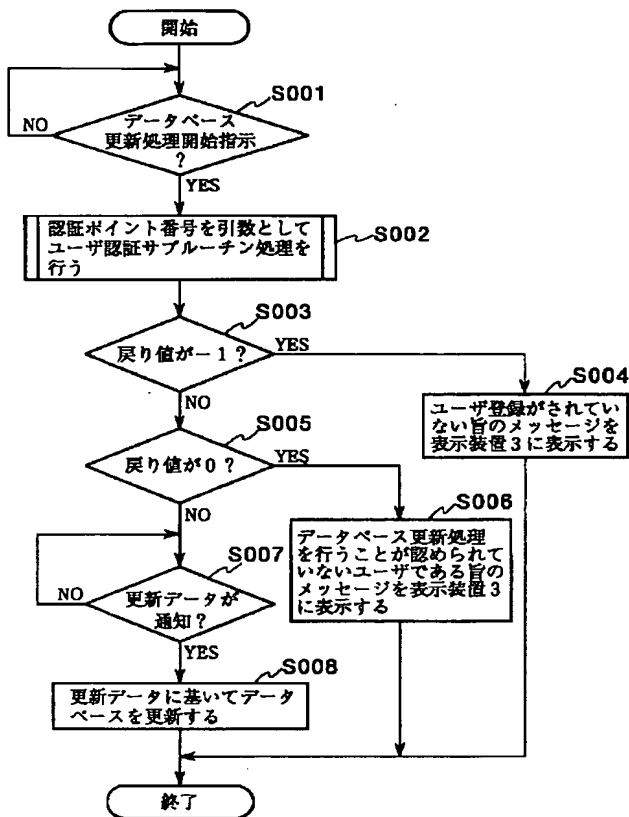
【図 2】



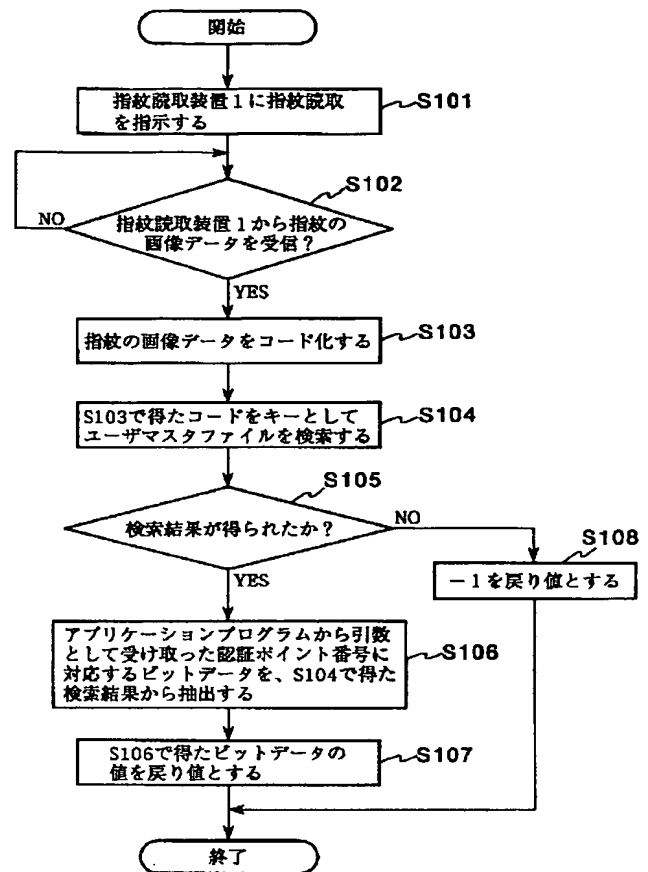
【図 3】



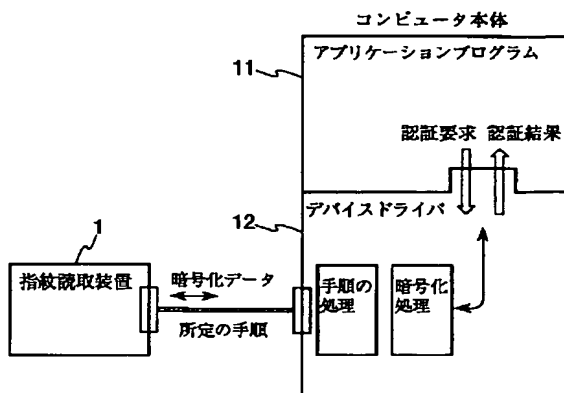
【図4】



【図5】



【図6】

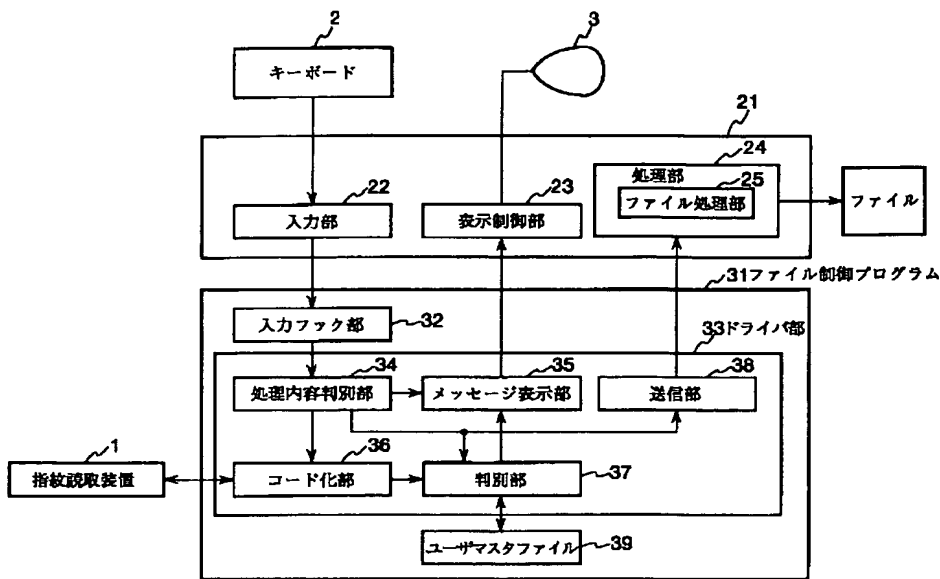


【図8】

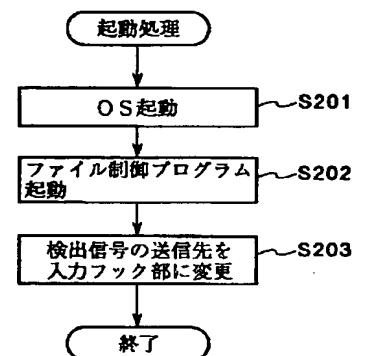
	ファイル1	ファイル2	ファイル3	.....	ユーザマスタファイル
A	○	○	×	.....	×
B	×	○	○	.....	×
...	.....	.....	.....	.....	.....
Z	○	○	○	.....	○

2: システム管理者

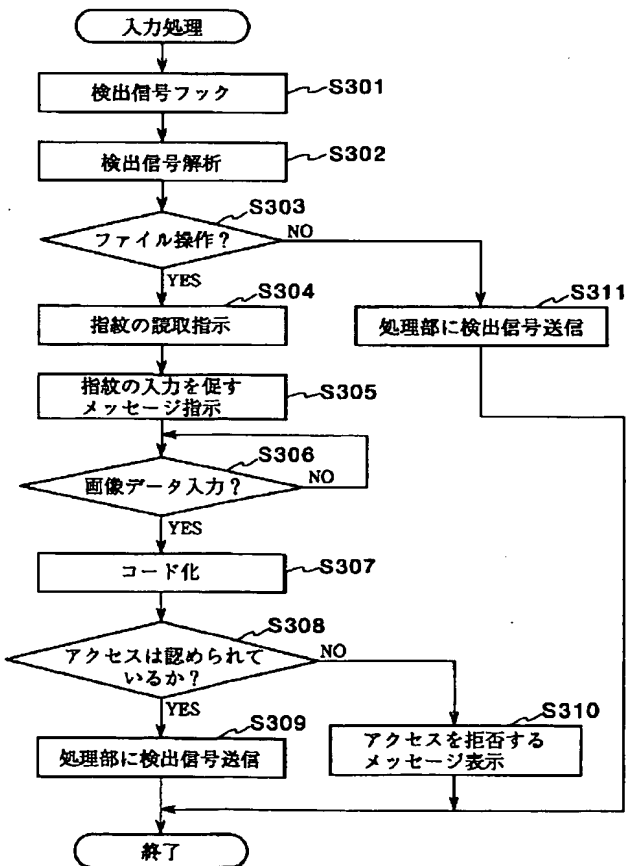
【図7】



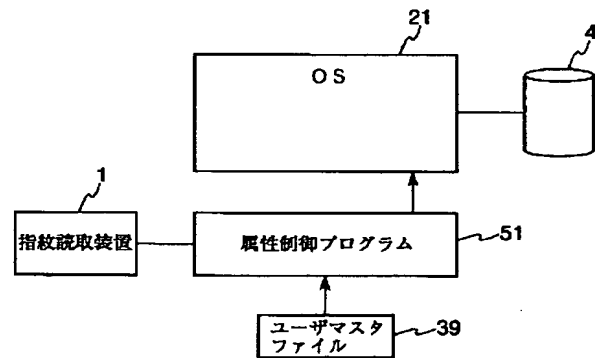
【図9】



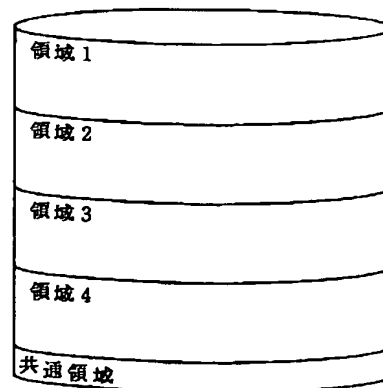
【図10】



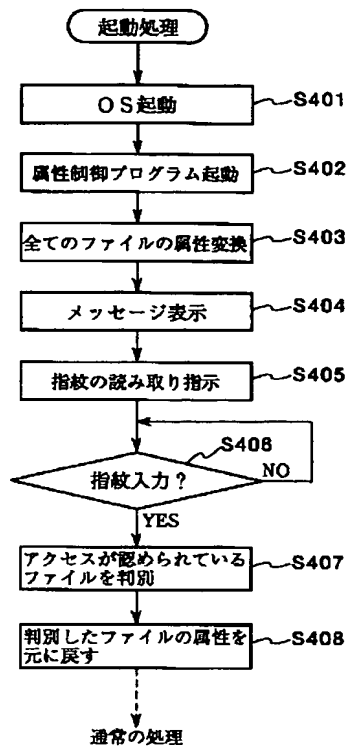
【図11】



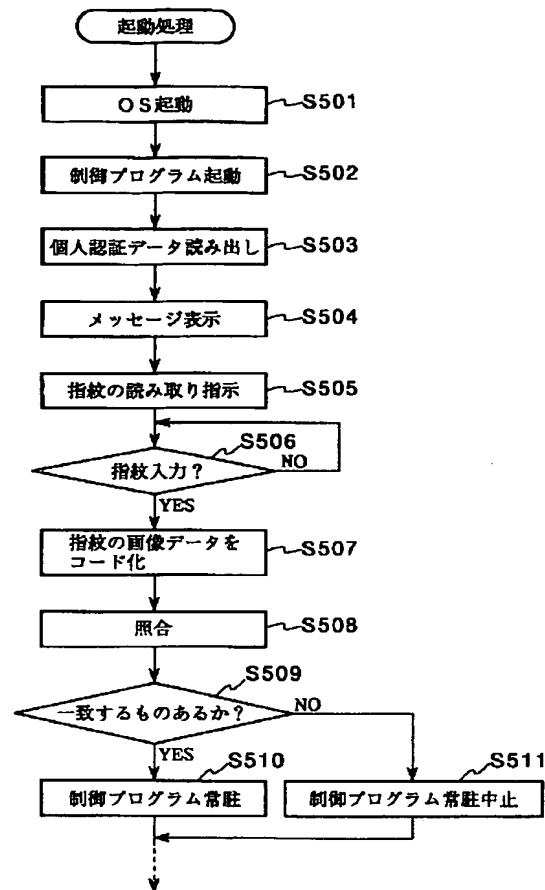
【図16】



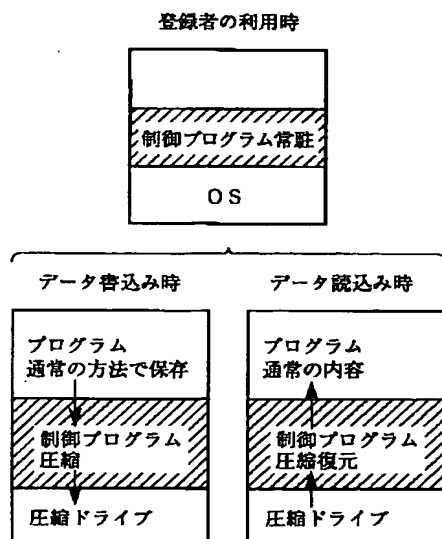
【図12】



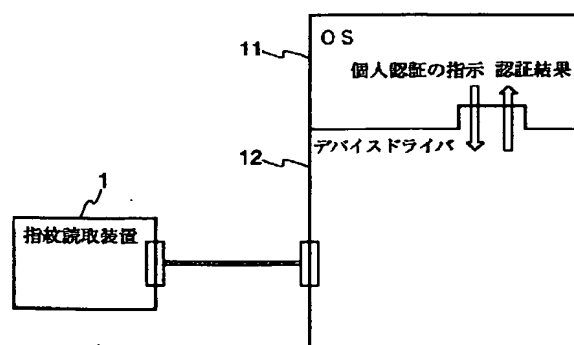
【図14】



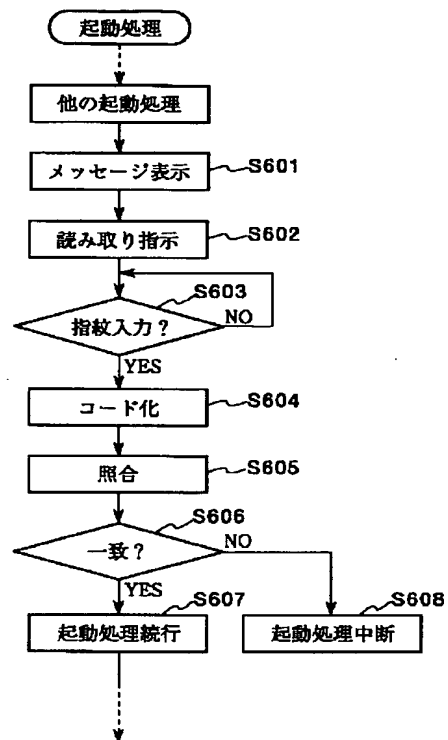
【図15】



【図17】



【図 18】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**